Axiom Sovereign

TECHNOLOGY SOVEREIGNTY ADVISORY

COMPLIANCE FRAMEWORK SERVICE — ASSESSMENT TOOL

NIST CSF 2.0 Maturity Scoring Worksheet

All Six Functions · Category-Level Scoring · Gap Analysis

v1.0 — 2026

Axiom Sovereign LLC · Severna Park, MD · info@axiomsovereign.com · axiomsovereign.com

NIST CSF 2.0 Maturity Scoring Worksheet

About NIST CSF 2.0 and This Worksheet

The NIST Cybersecurity Framework 2.0 (published February 2024) is the most widely adopted cybersecurity framework in the United States. It organizes cybersecurity activities into six Functions — Govern, Identify, Protect, Detect, Respond, and Recover — and provides a structured approach to understanding, assessing, and improving cybersecurity posture. This worksheet provides a maturity scoring tool aligned to all six Functions and their key Categories, producing a scored baseline you can track over time.

Maturity Scale

Level 1 — Initial: Practices are ad hoc, often reactive. Limited awareness of cybersecurity risk. Minimal documentation.

Level 2 — Developing: Some practices are in place but inconsistently applied. Awareness exists but not formalized. Some documentation.

Level 3 — Defined: Practices are documented, consistently applied, and communicated. Approved policies and procedures exist.

Level 4 — Managed: Practices are measured and monitored. Metrics tracked. Management uses data to make security decisions.

Level 5 — Optimizing: Continuous improvement based on lessons learned. Proactive adaptation to emerging threats. Program matures over time.

GOVERN (GV) — NEW IN CSF 2.0

The Govern function addresses organizational context, risk management strategy, roles and responsibilities, policy, oversight, and supply chain risk. It is the foundation for all other functions.

Category	Description	Current Maturity (1–5)	Target Maturity (1–5)	Gap	Priority Actions
GV.OC Organizational Context	Understand organizational mission, stakeholders, legal requirements, and the role of cybersecurity in business risk management.				

Category	Description	Current Maturity (1–5)	Target Maturity (1–5)	Gap	Priority Actions
GV.RM Risk Management Strategy	Establish, communicate, and monitor organizational cybersecurity risk management strategy and risk appetite.				
GV.RR Roles, Responsibilities, Authorities	Define, communicate, and enforce cybersecurity roles and accountability across the organization.				
GV.PO Policy	Establish, communicate, and enforce cybersecurity policy aligned to organizational context and risk strategy.				
GV.OV Oversight	Outcomes of organization-wide cybersecurity risk management are monitored and used to inform the risk management strategy.				
GV.SC Cybersecurity Supply Chain Risk Management	Cyber supply chain risk management processes are identified, established, managed, monitored, and improved.				

IDENTIFY (ID)

The Identify function develops an understanding of the organization's assets, business environment, governance, risk, and supply chain risk.

Category	Description	Current Maturity (1–5)	Target Maturity (1–5)	Gap	Priority Actions
ID.AM Asset Management	Maintain inventory of physical devices, software, systems, data, personnel, and external partners. Know what you have.				
ID.RA Risk Assessment	Identify, analyze, and prioritize cybersecurity risk to the organization, assets, and individuals.				
ID.IM Improvement	Identify improvements to organizational cybersecurity risk management processes, procedures, and activities.				

PROTECT (PR)

The Protect function develops and implements appropriate safeguards to ensure delivery of critical services.

Category	Description	Current Maturity (1–5)	Target Maturity (1–5)	Gap	Priority Actions
PR.AA Identity Management, Authentication, and Access Control	Identity and credentials are issued, managed, verified, revoked, and audited. MFA, least privilege, privileged access controls.				
PR.AT Awareness and Training	Personnel are provided with cybersecurity awareness and training commensurate with their role.				
PR.DS Data Security	Data are managed consistent with risk strategy to protect confidentiality, integrity, and availability. Encryption, DLP, classification.				
PR.PS Platform Security	Hardware, software, and services are managed consistent with risk strategy. Patching, configuration management, secure defaults.				
PR.IR Technology Infrastructure Resilience	Security architectures are managed with organizational risk strategy to protect asset and data integrity, availability, and confidentiality.				

DETECT (DE)

The Detect function develops and implements appropriate activities to identify cybersecurity events.

Category	Description	Current Maturity (1–5)	Target Maturity (1–5)	Gap	Priority Actions
DE.CM Continuous Monitoring	Systems and assets are monitored to identify cybersecurity events and verify effectiveness of protective measures.				
DE.AE Adverse Event Analysis	Anomalies and events are detected and their potential impact is analyzed. Correlation of events across systems.				

RESPOND (RS)

The Respond function develops and implements appropriate activities to act on a detected cybersecurity incident.

Category	Description	Current Maturity (1–5)	Target Maturity (1–5)	Gap	Priority Actions
RS.MA Incident Management	Responses to detected cybersecurity incidents are managed. Incident classification, triage, escalation.				
RS.AN Incident Analysis	Investigation is conducted to ensure effective response and support forensics and recovery.				
RS.CO Incident Response Reporting and Communication	Response activities are coordinated with internal and external stakeholders as required.				
RS.MI Incident Mitigation	Activities are performed to prevent expansion of an event, mitigate its effects, and document lessons learned.				

RECOVER (RC)

The Recover function develops and implements appropriate activities to maintain plans for resilience and restore capabilities.

Category	Description	Current Maturity (1–5)	Target Maturity (1–5)	Gap	Priority Actions
RC.RP Incident Recovery Plan Execution	Restoration activities are performed to ensure operational availability. Recovery plan tested and maintained.				
RC.CO Incident Recovery Communication	Restoration activities are coordinated with internal and external parties including coordinating centers and ISPs.				

MATURITY SCORE SUMMARY

CSF Function	Categories	Avg Current Maturity	Avg Target Maturity	Gap	Priority
Govern (GV)	6				
Identify (ID)	3				
Protect (PR)	5				
Detect (DE)	2				
Respond (RS)	4				

CSF Function	Categories	Avg Current Maturity	Avg Target Maturity	Gap	Priority
Recover (RC)	2				
OVERALL	22				

Scoring interpretation: An overall average of 3.0+ across all functions indicates a defined, consistent program. Most mid-market organizations score 1.5–2.5 at initial assessment. A target of 3.0–3.5 is appropriate for most professional services organizations and satisfies the expectations of most cyber insurers and enterprise procurement teams.

Ready to Get Started?

Schedule your complimentary 30-minute discovery call: calendly.com/cmissimore-6zkc/30min
info@axiomsovereign.com · axiomsovereign.com